21. Active Directory - Forensics

🧠 1. Foundational Understanding of Active Directory

Concept	Description
Active Directory (AD)	A centralized directory service by Microsoft used to authenticate and authorize users and computers in a Windows domain network.
Key Components	Domains, Domain Controllers (DCs), Organizational Units (OUs), Group Policy Objects (GPOs), Users, Computers.
Purpose	Centralized management of users, systems, security policies, and access control.

📌 **Why it matters**: Since AD controls access across an enterprise, it's a prime target for attackers.

🔍 2. Role of Forensics in Active Directory

Forensics in AD involves:

- Investigating incidents involving unauthorized access, privilege escalation, and lateral movement.
- Analyzing logs and artifacts on **Domain Controllers**, workstations, and servers.

🎯 Goals:

- Identify **initial access** point
- Trace the **attack path**
- Understand the **intent and scope** of the attack
- Collect evidence for remediation and legal response

🛑 3. Detecting Suspicious Activity in AD Logs

🔎 Key Log Sources:

Log Location	Type
Security Logs	Authentication, privilege use, account changes
Directory Service Logs	LDAP queries, replication issues
Sysmon Logs (optional)	Process creation, network connections
DNS Server Logs	Reconnaissance activities
Event Forwarding	Centralized log collection across machines

📜 4. Critical Windows Event IDs to Know

Event ID	Description	Suspicious When...
4624	Successful logon	Logon type 3 (network) from strange IP
4625	Failed logon	Multiple failures could mean brute-force
4672	Special privileges assigned	Logged when admin rights are used
4648	Logon with explicit credentials	Could show lateral movement
4768/4769	Kerberos ticket requests	Spikes may indicate Kerberoasting
4720/4722/4723	User account creation/reset	Especially if outside normal admin hours
4740	Account locked out	Could indicate password spraying
5140/5145	Access to shared objects	Unauthorized access to file shares
4662	Object permissions changed	Could show privilege escalation or backdoors

🔬 5. Analyzing Logs for Malicious Activity

🔑 Focus areas:

- **Unusual logon times**
- **Logon attempts from different locations in quick succession**
- **Creation of backdoor accounts**
- **Unusual Group Membership Changes** (e.g., user added to Domain Admins)
- **Mass ticket requests** (indicative of ticket harvesting)

📂 Tools:

- Event Viewer
- PowerShell (`Get-WinEvent`, `Get-EventLog`)
- Log analyzers like Splunk, ELK, or Graylog

📖 6. Extracting and Interpreting Log Data

Step	What to Extract
✅ **Source IP/Hostname**	Origin of logon or attack
✅ **User Account**	Used for action

Step	What to Extract
✅ **Process or Service**	e.g., `lsass.exe`, `powershell.exe`
✅ **Time**	Timestamps to correlate across logs
✅ **Domain Controller Name**	Where the event was recorded

🧩 7. Methodical Investigation Approach

🧭 A structured plan for AD forensics:

1. **Baseline Normal Activity** – Know what's expected
2. **Detect Anomalies** – Unusual accounts, access, or logons
3. **Correlate Events** – Use multiple sources (Security logs + Sysmon + DNS)
4. **Timeline Creation** – Build a detailed timeline of events
5. **Evidence Preservation** – Export logs, disk images if needed
6. **Analysis and Reporting** – Document every finding with timestamps, users, actions, and suspected impact

---

📝 8. Documentation and Reporting

Key elements to include in forensic reporting:

- **Executive Summary** – What happened, when, and impact
- **Technical Details** – IPs, accounts, timestamps, event IDs
- **Indicators of Compromise (IoCs)** – e.g., hashes, domains, tools used
- **Timeline of Events**
- **Recommendations** – Fixes, patches, policy updates
- **Screenshots / Log Excerpts**

📄 Reporting Tools:

- Markdown, Word, or PDF formats
- Case management tools (TheHive, Velociraptor, etc.)

🚀 Final Thoughts

Learning AD forensics helps you:

- Defend your enterprise by detecting early signs of compromise.
- Understand the **attacker's footprint**.
- Respond quickly with precision and clarity.